УДК 004.056.5

В. Ф. ГОЛИКОВ, М. Л. РАДЮКЕВИЧ

ФОРМИРОВАНИЕ ОБЩЕГО СЕКРЕТА С ПОМОЩЬЮ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Белорусский национальный технический университет
Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»

В работах [1–3] предлагается использование двух синхронизируемых искусственных нейронных сетей (СИНС), соединенных открытым каналом связи для конфиденциального формирования общего криптографического ключа. В [3] рассматриваются возможности по формированию такого же ключа третьей стороной, прослушивающей канал связи и синхронизирующей свою сеть. Вместе с тем, остаются мало исследованными вопросы практической пригодности данной технологии для ответственных криптографических приложений. Отсутствуют рекомендации по выбору параметров используемых сетей, обеспечения приемлемого быстродействия и гарантированной конфиденциальности сформированного общего секрета.

В связи с этим представляет интерес обоснование рациональных значений параметров ИНС с точки зрения криптографических требований и анализ безопасности предлагаемого способа формирования криптографических ключей.

Ключевые слова: *синхронизируемые искусственные нейронные сети, атака, общий криптографический ключ, параметры искусственных нейронных сетей.*

Введение

Абоненты *A* и *B*, имеют идентичные ИНС, соединенные открытым каналом связи [1, 2] (рис. 1). Каждая ИНС, состоит из одного слоя персептронов. Каждый персептрон имеет *n* входов и прямоугольную функцию активации σ(*) (рис. 2).

До начала синхронизации абоненты *A* и *B* независимо друг от друга формируют вектор весовых коэффициентов (*ВК*)

$$\bar{w}\mathrm{a} = wa_{11},\ wa_{12}, \ldots, wa_{1n}, wa_{21}, wa_{22}, \ldots, wa_{2n}, \ldots, wa_{K1},\ wa_{K2},\ \ldots,\ wa_{Kn}, \quad (1)$$

$$\bar{w}b = wb_{11},\ wb_{12}, \ldots, wb_{1n},\ wb_{21},\ wb_{22}, \ldots, wb_{2n}, \ldots,\ wb_{K1}, wb_{K2}, \ldots, wb_{Kn}, \quad (2)$$

где wa_{ij}, $wb_{ij} \in [-L, L]$, $i = 1, 2, ..., K$; $j = 1, 2, ..., n$; L – целое число.

Каждый элемент этих векторов w_{ij} есть случайное целое число с дискретным равномерным законом распределения (рис. 3)

$$P(w_{ij} = s_{ij}) = \frac{1}{2L+1},$$

где $s_{ij} = -L, -L+1, \ldots, -1, 0, 1, \ldots, L-1, L$.

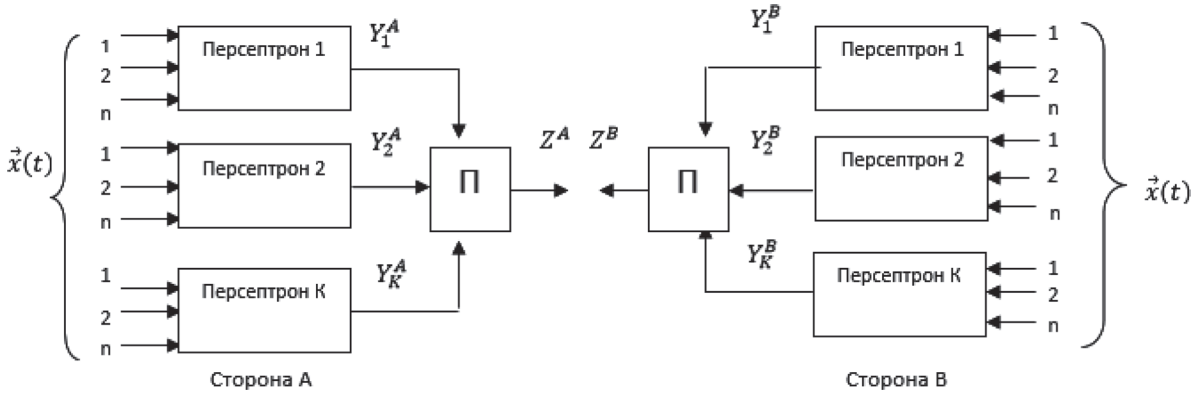

Рис. 1. Синхронизируемые ИНС

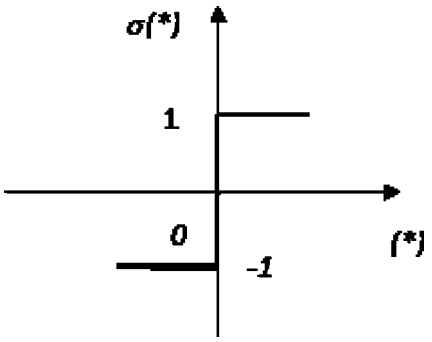

Рис. 2. Функция активации

Каждый шаг синхронизации начинается с подачи на входы обеих сетей выбранного случайным образом вектора

$$\vec{x}(t) = x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, \ldots, x_{K1}, x_{K2}, \ldots, x_{Kn}, \quad (3)$$

где $x_{ij} \in [-1, 1]$ – дискретная случайная величина с равномерным распределением, $t = 1, 2, \ldots$ – номер такта (далее все рассматриваемые величины зависят от t, но для упрощения записи эта зависимость в обозначениях отсутствует).

Для каждого персептрона выходная величина равна

$$Y_i^{A/B} = \sigma\left(\sum_{j=1}^{n} w_{ij}^{A/B} x_{ij}\right) \quad (4)$$

Индекс A/B означает, что операция касается обеих сетей A и B, а единичный индекс – что операция касается одной сети соответственно. Функция активации $\sigma(*)$ имеет вид

$$\sigma(*) = \begin{cases} 1, \ \sigma(*) \geq 0, \\ -1, \ \sigma(*) < 0. \end{cases} \quad (5)$$

Затем вычисляется выходная величина Z для каждой из сетей

$$Z^{A/B} = \prod_{i=1}^{K} Y_i^{A/B} = \prod_{i=1}^{K} \sigma\left(\sum_{j=1}^{n} w_{ij}^{A/B} x_{ij}\right) \quad (6)$$

На основании сравнения обоих полученных выходных величин реализован процесс синхронизации. Коррекция векторов весов обеих сетей происходит только тогда, когда обе выходные величины равны друг другу ($Z^A = Z^B$). Внутри данной сети корректируются веса только тех персептронов, выходная величина которых равна величине Z всей сети. Процесс коррекции идет по правилу Хэбба

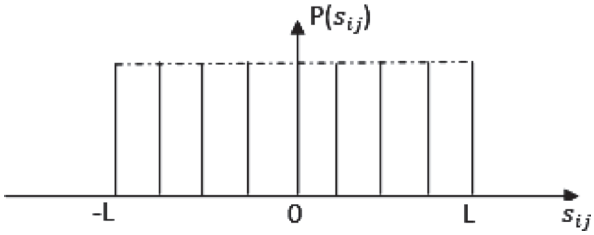

Рис. 3. Закон распределения начальных значений весовых коэффициентов

$$w_{ij}^{A/B} = \begin{cases} w_{ij}^{A/B} + Z^{A/B} x_{ij}, \text{ если } Z^A = Z^B \text{ и } Z^{A/B} = Y_i^{A/B}, \\ w_{ij}^{A/B}, \text{ в противном случае.} \end{cases}$$

Кроме того, учитывается ограничение $w_{ij}^{A/B} \in [-L, L]$

$$w_{ij}^{A/B} = \begin{cases} \pm L, & \text{если } \left|w_{ij}^{A/B}\right| > L, \\ w_{ij}^{A/B}, & \text{в противном случае.} \end{cases}$$

Процесс синхронизации продолжается до полного совпадения векторов $\bar{w}a, \overline{wb}$, после чего абоненты A и B имеют общую секретную информацию, представляющую собой последовательность десятичных чисел вида

$$\bar{w}^{A/B} = w_{11}, w_{12}, \ldots, w_{1n}, w_{21}, w_{22}, \ldots, w_{2n}, \ldots, w_{K1}, w_{K2}, \ldots, w_{Kn}. \quad (7)$$

Общее секретное число можно сформировать из (7), например, как конкатенацию значений ВК

$$S = w_{11} \| w_{12} \| \ldots \| w_{1n} \| w_{21} \| w_{22} \| \ldots \| w_{2n} \| \ldots \| w_{K1} \| w_{K2} \| \ldots \| w_{Kn}. \quad (8)$$

1. Статистические закономерности процесса синхронизации

1.1. Неопределенность момента наступления полной синхронизации

В процессе синхронизации ИНС обмениваются через открытый канал связи только выходными величинами сетей $Z^{A/B}$, поэтому не знают равны ли ВК их сетей или нет. Следовательно, они не знают, нужно ли им продолжать цикл синхронизации или можно остановиться.

Неопределенность относительно наступления полной синхронизации ВК для абонентов приводит к тому, что процесс синхронизации может продолжаться уже после выравнивания

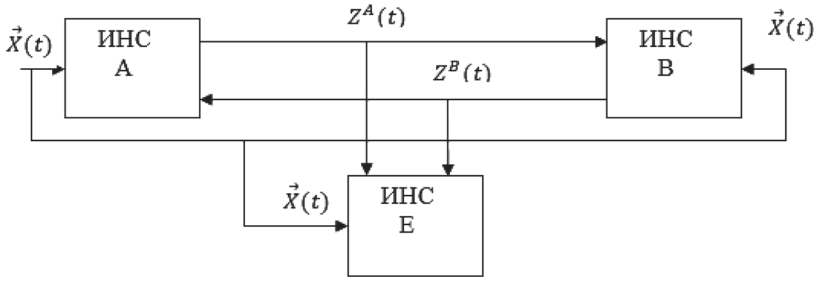

Рис. 4. Схема взаимодействия сетей: t – номер такта синхронизации, $\vec{X}(t)$ – вектор синхронизирующих случайных воздействий, $Z^A(t)$, $Z^B(t)$ – выходные величины сетей A и B соответственно

ВК. Это с одной стороны увеличивает время формирования общего ключа и повышает шансы злоумышленника на реализацию возможных атак [3], с другой – могут иметь место случаи преждевременной остановки процесса синхронизации. В [4] предложен способ определения момента наступления полной синхронизации, основанный на том, что после наступления полной синхронизации выходные величины сетей всегда равны. Поэтому, если в процессе синхронизации наблюдается длительное равенство выходных величин сетей, то есть основания полагать о наступлении полной синхронизации. Экспериментальное исследование, приведенное с помощью имитационной модели [4], показало, что в процессе синхронизации пока $\vec{w}^A(t) \neq \vec{w}^B(t)$, наблюдаются такты, в которых $Z^A(t) \neq Z^B(t)$, и такты, в которых $Z^A(t) = Z^B(t)$. Действительно, как показали эксперименты, довольно часто встречаются отрезки тактов длиной до нескольких сотен и более совпадений $Z^A(t) = Z^B(t)$, однако синхронизация еще не достигнута. Таким образом, решение этой задачи носит вероятностный характер и базируется на результатах имитационного моделирования. Так или иначе, но процесс формирования общего ключа должен заканчиваться сравнением $\vec{w}^A(t_c)$ и $\vec{w}^B(t_c)$, чтобы A и B были уверены в идентичности полученных результатов. Эта процедура может выполняться с применением хэширования, т. е. сравниваются хэш-значения векторов $h\left[\vec{w}^A(t_c)\right]$ и $h\left[\vec{w}^B(t_c)\right]$ или шифрованием и расшифрованием отрывка текста, с использованием в качестве ключей вышеуказанных векторов.

Наряду с проблемой своевременной остановки процесса синхронизации существует проблема выбора параметров СИНС: K, n, L. Выбор этих параметров необходимо произвести исходя из криптографических соображений, имея ввиду конфиденциальность сформированного ключа и время формирования т. е. количество тактов синхронизации, потраченных на это. Поскольку эти характеристики зависят [3] от параметров сетей и моделей поведения третьей стороны E, пытающейся узнать значение ключа, то далее следует рассмотреть статистические закономерности процесса синхронизации при наличии криптоаналитика E.

1.2. Модели поведения криптоаналитика

Рассмотрим основные известные атаки на формируемый ключ со стороны третьей стороны, «прослушивающей» канал связи, по которому синхронизируемые сети обмениваются информацией.

Схема взаимодействия сетей абонентов и криптоаналитика представлена на рис. 4.

Архитектура и параметры всех сетей идентичны (рис. 1).

1.2.1. Силовая атака

Силовая атака, также известная как полный перебор – метод взлома, являющийся самым универсальным, однако и самым долгим. Относится к классу методов поиска решения исчерпыванием всевозможных вариантов. Сложность полного перебора зависит от количества всех возможных значений формируемого ключа.

Для того чтобы оценить эффективность силовой атаки, необходимо рассчитать количество всевозможных значений всей совокупности весовых коэффициентов. Всевозможное количество значений рассчитывается по формуле:

$$n = \left(2L+1\right)^{n*K} \qquad (9)$$

Для количественной оценки выберем нейросеть с параметрами $n = 25$, $K = 3$, $L = 8$. Подставляя соответствующие значения в формулу, получим количество комбинаций, равное

$1{,}9 \cdot 10^{92}$. При скорости перебора, равной 1 миллиарду комбинаций в секунду, на полный перебор всех комбинаций уйдет $6{,}02 \cdot 10^{75}$ лет, что намного больше предположительного времени актуальности зашифрованной информации. Из этого следует, что данный метод не подходит для взлома, даже при относительно небольших значениях параметров сети.

1.2.2. Простая атака

При простой атаке для взлома ключа криптоаналитику необходимо иметь свою собственную нейросеть, имеющую такую же структуру, как и сети легитимных абонентов.

При начале сеанса выработки ключа криптоаналитик подключает свою сеть к каналу связи, и, при помощи перехватываемых векторов синхронизирующих случайных воздействий и выходных величин сетей A и B, обучает сеть E по следующим правилам обучения:

1) Если сети A и B получили разные выходные величины $(Z^A \neq Z^B)$, то сеть E не меняет своих весов.

2) Если сети легитимных пользователей получили одинаковые выходные величины $(Z^A = Z^B)$ и к тому же выходная величина оппонента E равна выходным величинам наблюдаемых сетей $(Z^A = Z^B = Z^E)$, то сеть E производит коррекцию своих ВК.

3) Если выходы обеих сетей согласованы $(Z^A = Z^B)$, а криптоаналитик E получает другую выходную величину $(Z^A = Z^B \neq Z^E)$, то сеть E пропускает коррекцию, так как ее пропускают сети A и B.

Это приводит к тому, что количество коррекций сети E оказывается меньше, чем количество коррекций ИНС у A и B и это приводит к задержке в процессе обучения сети оппонента относительно времени синхронизации наблюдаемых сетей. Это отставание является главным элементом безопасности процесса синхронизации. Если процесс синхронизации завершится на довольно раннем этапе, то оппонент будет не в состоянии синхронизировать свои вектора весов с наблюдаемыми сетями. Следовательно, чем больше эта задержка, тем выше уровень безопасности.

1.2.3. Геометрическая атака

Для ослабления эффекта отставания в количестве коррекций применяется атака под названием геометрическая. При возникновении случая 3, т. е. при $(Z^A = Z^B \neq Z^E)$, делается предварительная коррекция, выходной величины того персептрона сети E, у которого величина $\sum_{i=1}^{n} w_{ij}^E x_{ij}$ наименьшая по абсолютному значению. Это приводит к изменению знака выбранного персептрона на противоположный, аналогично и знака всей сети, что переводит сеть в случай 2. Эффективность такой атаки в среднем выше чем эффективность простой атаки, поэтому в дальнейшем будем считать основной моделью поведения E.

1.3. Конфиденциальность сформированного общего ключа

Так как процессы синхронизации, протекающие в рассматриваемых сетях, являются случайными, то и исследование должно проводится с использованием математических вероятностных моделей.

Обозначим количество назначенных тактов синхронизации через d, количество фактических тактов синхронизации до достижения равенства ВК сетей A и B через t_{AB}, а сетей A и E через t_{AE}. Величины t_{AB} и t_{AE} – дискретные случайные величины, законы распределения которых зависят от параметров сетей L, n, K. В некоторых источниках, например [5], для оценки уровня безопасности процесса синхронизации в рассматривается параметр, названный коэффициентом безопасности $r = T_{AE} / T_{AB}$, где T_{AB} – среднее время до полной синхронизации сетей A и B, T_{AE} – среднее время до полной синхронизации сетей A и E. С помощью этого параметра можно проследить тенденцию зависимости безопасности от параметров сети. Однако для криптографических применений важна не безопасность в среднем, а конкретно в каждом сеансе формирования, поэтому далее рассматриваются другие критерии.

В процессе синхронизации могут произойти следующие события:

1. Сети A и B достигли синхронизма (их веса стали равны друг другу), E смог обучить свою сеть. Для этого события выражение вероятности запишется в виде $P(t_{AB} \le d, t_{AE} \le d)$. Это событие является неблагоприятным, так как сформированный ключ сразу дискредитируется.

2. Сети A и B достигли синхронизма, E не успел обучить свою сеть. Для этого события

выражение вероятности запишется в виде $P(t_{AB} \le d, t_{AE} > d)$. Это событие является благоприятным, так как ключ был сформирован и не дискредитирован.

Остальные события нас не интересуют, так как в случае их наступления A и B не достигают синхронизма, следовательно, ключ не будет сформирован.

Вероятность сложного события ($t_{AB} \le d$, $t_{AE} \le d$), пренебрегая взаимосвязью частных событий можно представить следующим образом:

$$P\left(t_{AB} \le d, t_{AE} \le d\right) = \\ = P\left(t_{AB} \le d\right) P(t_{AE} \le d / t_{AB} \le d) \approx \\ \approx P\left(t_{AB} \le d\right) P\left(t_{AE} \le d\right). \quad (10)$$

По аналогии преобразуется выражение $P(t_{AB} \le d, t_{AE} > d)$. Данные преобразования позволяют нам перейти к одномерным вероятностям, что упрощает расчетную часть.

Исходя из выше описанных правил, задача анализа безопасности сводится к расчету вероятности удачной синхронизации сетей A и B $\left(P(t_{AB} \le d)\right)$, а также удачной либо неудачной попытки обучения сети E $\left(P(t_{AE} \le d), P(t_{AE} > d)\right)$ при выбранных значениях d.

Аналитический расчет этих вероятностей не представляется возможным из-за высокой сложности. Поэтому расчет проводился методом статистического моделирования. Для этого была разработана программная модель СИНС и сети криптоаналитика E. С помощью этой модели была имитирована реальная синхронизация. Повторяя этот процесс многократно, вычислены статистические значения искомых вероятностей для различных параметров сетей.

Исследования показали, что независимо от вида атаки обеспечивается

$$P(t_{AB} \le d) > P(t_{AE} \le d) \quad (11)$$

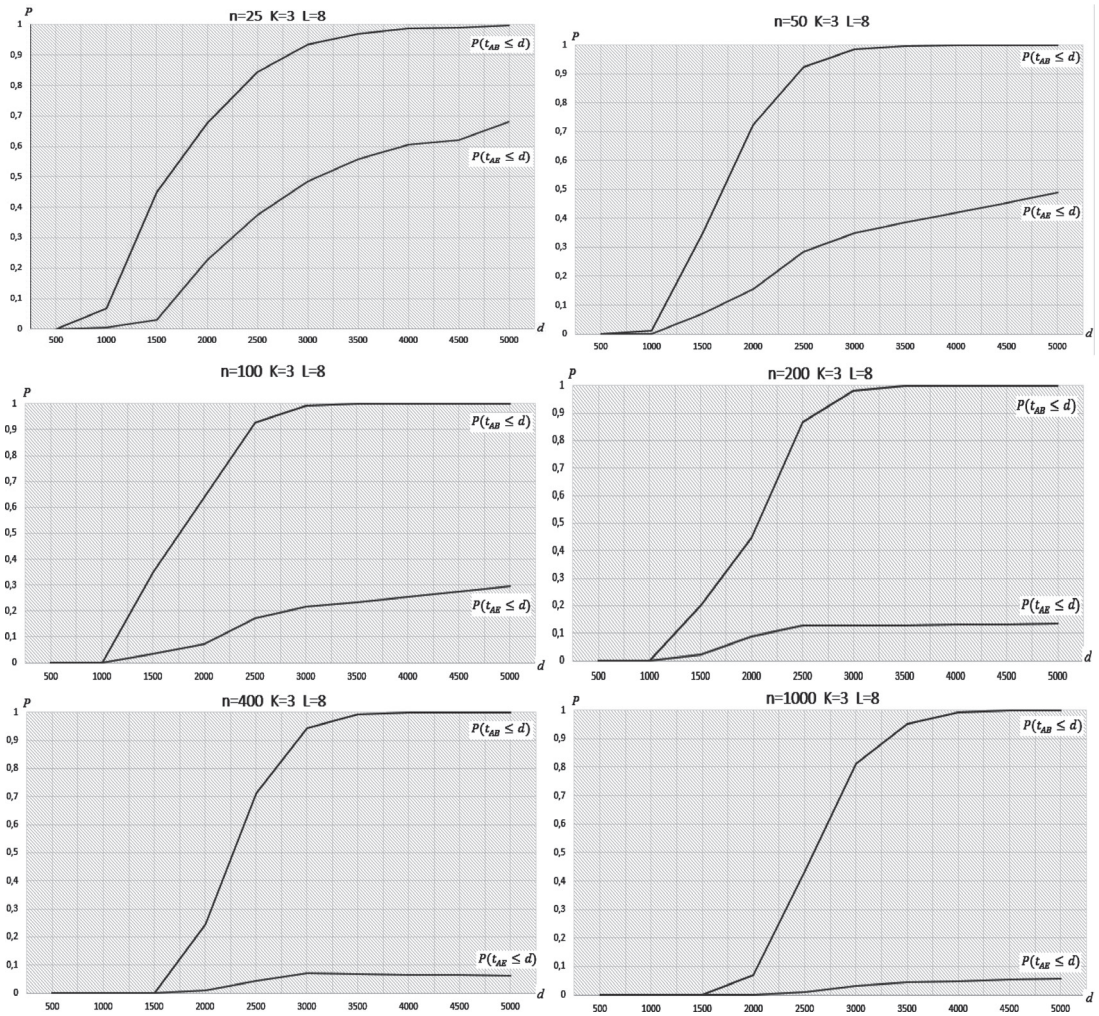

Рис. 5. Результаты имитационного моделирования

Выражение (11), однако, совсем не означает, что в процессе атаки обязательно произойдет событие $t_{AB} \le d \le t_{AE}$. Т. е. могут иметь место успешные атаки, при которых окажется $t_{AE} \le t_{AB} \le d$. С наличием таких реализаций и связаны основные сомнения в безопасности анализируемого метода открытого формирования общего секрета.

На рис. 5 приведены вероятности $P(t_{AE} \le d)$, полученные методом имитационного моделирования при некоторых значениях параметров сетей. Анализируя результаты моделирования, полученные авторами статьи и другими исследователями [3], можно выявить важные закономерности, которые могут быть использованы для принятия конкретных решений.

2. Выбор параметров и обоснование структуры ИНС

Анализ результатов моделирования и работ других авторов позволяет сформулировать предложения по обоснованию структуры и параметров СИНС.

Решение этой задачи, на наш взгляд, следует начать с выбора диапазона значений ВК, который вместе с количеством входов n и числом персептронов K задает с одной стороны множество возможных значений $\bar{w}^{A/B}$, с другой сильно влияет на длительность процесса согласования ВК сетей A и B. Увеличение L приводит к увеличению множества возможных значений $\bar{w}^{A/B}$, т. е. к увеличению криптостойкости, но при этом увеличивается длительность процесса согласования ВК, т. е. снижается скорость работы алгоритма. С точки зрения обеспечения требуемой криптостойкости следует отдать предпочтение первому фактору. Поэтому величину L будем выбирать исходя из криптографических факторов.

В результате полной синхронизации A и B формируют общую последовательность десятичных чисел (8), состоящую из целых положительных и отрицательных чисел из интервала $[-L, L]$. Для использования этой последовательности чисел в качестве криптографического ключа ее следует преобразовать в бинарную.

Возникает вопрос о выборе разрядности двоичного числа при переходе от десятичного формата ВК к двоичному. Как уже указывалось выше, диапазон изменения значений десятичных чисел w_{ij} задается величиной L и равен $[-L, L]$. Таким образом, количество возможных значений w_{ij} равно $2L + 1$. Двоичным числом длиной l можно описать 2^l десятичных чисел, а так как $2L + 1$ нечетное число, то точное его описание для произвольно выбранных значениях L невозможно. Избыточная разрядность нежелательна, так как это приведет к избыточному количеству нулей в ключевой последовательности. Поэтому возможна следующая методика. Уменьшим количество возможных значений w_{ij} на единицу и вычислим необходимую разрядность l:

$$2L = 2^l, \text{ откуда } l = \ln(2L). \qquad (12)$$

В табл. 1 приведены значения L и соответствующие значения l.

Таблица 1. **Соответствие разрядности двоичного числа десятичному**

L	2	4	8	16	32
l	2	3	4	5	6

Тогда таблица для перевода десятичных чисел в двоичные, например, для $L = 4$ имеет вид в табл. 2.

Таблица 2. **Перевод десятичного числа в двоичное**

$w_{ij(10)}$	0	1	2	3	4	–1	–2	–3	–4
$w_{ij(2)}$	000	001	010	011	100	101	110	111	–

Из последней таблицы видно, что трехразрядных чисел не хватает для замены всех десятичных чисел выбранного интервала. Замена на одно из уже используемых двоичных чисел возможна, но нежелательна, так как это нарушает равномерность распределения чисел. Лучший вариант это переход на несимметричный интервал $[L_1, L_2]$ (для рассматриваемого случая: $L_1 = -3$, $L_2 = 4$), но при этом нужно изменить и функцию активации, сдвинув ее вправо на единицу рис. 6.

С учетом (12) длина сформированной секретной последовательности в битах равна

$$r_{(2)} = nK \ln(2L). \qquad (13)$$

Необходимую длину ключа, как следует, из (13) можно обеспечить соответствующим выбором n, K, L, учитывая при этом, что $d \le T$, где T – допустимое число тактов, отведенное на сеанс связи. Эксперименты показывают, что обеспечение необходимой величины $r_{(2)}$ це-

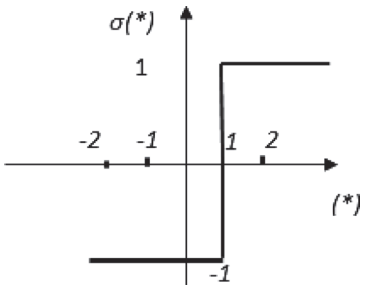

Рис. 6. Функция активации для несимметричного интервала

лесообразно обеспечивать выбором $n \geq 1000$ при $K = 3$, $L = 8$. При этом согласно графикам (рис. 6) обеспечивается $P(t_{AB} \leq d) = 0{,}994$, $P(t_{AE} \leq d) = 0{,}005$ при $d = 4000$ тактов. Увеличение L в 2 раза вызывает увеличение d примерно в 10 раз при некотором снижении величины $P(t_{AE} \leq d)$, к аналогичным результатам приводит и увеличение K. Таким образом, если выбрать: $n = 1000$, $K = 3$, $L = 8$, $d = 4000$, то можно с вероятностью $P(t_{AB} \leq d) = 0{,}994$ сформировать общую бинарную последовательность длиной $r_{(2)} = 12\,000$ битов, конфиденциальность которой не менее $P(t_{AE} \leq d) = 0{,}045$.

Возникает вопрос насколько достигнутые значения вероятностей удовлетворяют криптографическим требованиям. Вероятность $P(t_{AB} \leq d)$ является важной характеристикой, но не критичной, так как, если формирование общего ключа в данном сеансе не состоится, то его можно повторять до получения успеха. Другое дело с вероятностью $P(t_{AE} \leq d)$. Полученные цифры можно трактовать, как то, что из каждой 1000 сформированных ключей, криптоаналитик буде знать 45. В некоторых случаях такая конфиденциальность может оказаться недостаточной.

Заключение

Таким образом из рассмотренного можно сделать следующие выводы:

– при использовании СИНС для формирования общего секретного ключа необходимо исходить из приемлемых значений вероятностей $P(t_{AB} \leq d)$ и $P(t_{AE} \leq d)$;

– для обеспечения требуемой стойкости к возможным атакам следует выбирать: $L \geq 8$, $K \geq 3$, $n \geq 1000$.

ЛИТЕРАТУРА

1. **Kanter, I.** The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel.–2005. Vol. 5, n. 1. – P. 130–140.

2. **Kinzel, W.** Neural Cryptography / W. Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

3. **Ruttor, A.** Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.

4. **Голиков В. Ф., Брич Н. В., Пивоваров В. Л.** «О некоторых проблемах в задачах распределения криптографических ключей с помощью искусственных нейронных сетей», Системный анализ и прикладная информатика, № 1–3, 2014.

5. **Плонковски, М.** Криптографическое преобразование информации на основе нейросетевых технологии / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика; под ред. И. М. Жарского. – Минск: БГТУ, 2005.

REFERENCES

1. **Kanter, I.** The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel. – 2005. Vol. 5, n. 1. – P. 130–140.

2. **Kinzel, W.** Neural Cryptography / W. Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

3. **Ruttor, A.** Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.

4. **Golikov V. F., Brich N. V., Pivovarov V. L.** «On some problems in the distribution of cryptographic keys using artificial neural networks», System Analysis and Applied Informatics, № 1–3, 2014.

5. **Plonkovski, M.** Cryptographic transformation of information based on neural network technology / M. Plonkovski, P. P. Urbanovich // Proceedings of BSTU. Series VI. Physics and Mathematics and Informatics; by ed. I. M. Zharsky. – Minsk: BSTU, 2005.

HOLIKAU U. F., RADZIUKEVICH M. L.

GENERATION A SHARED SECRET USING ARTIFICIAL NEURAL NETWORKS

Belarusian National Technical University
Scientific Production Republican Unitary Enterprise «Research Institute for the Technical Protection of Information»

In the Kanter's and Kinsella's works is proposes the use of two synchronized artificial neural networks (SANN) connected by opening communication channel to confidential formation of a common cryptographic key. At the same time, there are few

questions of practical suitability of this technology for cryptographic applications. There are no recommendations on the choice of parameters of the used networks, ensuring acceptable speed and guaranteed confidentiality of the generated general secret.

In this regard, it is interesting to substantiate the rational values of the parameters of ANN from the point of view of cryptographic requirements and security analysis of the proposed method of formation of cryptographic keys.

Keywords: *synchronized artificial neural networks, attack, common cryptographic key, parameters of the synchronized artificial neural networks.*

Голиков Владимир Федорович

Доктор технических наук, профессор кафедры «Информационные технологии в управлении» Белорусского национального технического университета. Сфера научных интересов: защита информации, криптография.

E-mail: vgolikov@bntu.by

Радюкевич Марина Львовна

Магистр технических наук. Начальник испытательной лаборатории по требованиям безопасности информации научно-производственного республиканского унитарного предприятия «Научно-исследовательский институт технической защиты информации». Победитель конкурса молодых ученых на XXIV научно-практической конференции «Комплексная защита информации».

E-mail: 1218a@list.ru